ISO/CDC11231

Fourth Draft Issue

Date 2006-04-24

ISO/TC 20/SC 14/WG 5

Probabilistic Risk Assessment

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International standard
Document subtype: if applicable
Document stage: (20) Preparation
Document language: E

Draft 2004-04-08

Contents

Page

Figures

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electro-technical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

ISO 16193 was prepared by Technical Committee ISO/TC 20, *Aircraft and Space Vehicle*, Subcommittee SC 14, *Space systems and operations*, Working Group 5. This technical standard is the first issue of an ISO standard concerning Probabilistic Risk Assessment (PRA).

Introduction

Structured risk management processes use qualitative and quantitative risk assessment techniques to support optimal decisions regarding safety and the likelihood of mission success as provided for in ISO17666. The most systematic and comprehensive methodology for conducting these evaluations is probabilistic risk assessment (PRA).

Probabilistic Risk Assessment has, over the past three decades, become the principal analytic method for identifying and analyzing risk from project and complex systems. Its usefulness for Risk Management (RM) has been proven in many industries including aerospace, electricity generation, petrochemical, and defense. PRA is methodology used to identify and evaluate risk to facilitate RM activities by identifying dominant contributors to risk so that resources can be effectively allocated to address significant risk drivers and not wasted on items that contribute insignificantly to the risk. In addition to analyzing risk, PRA provides a framework to quantify uncertainties in events and event sequences that are important to system safety. By enabling the quantification of uncertainty, PRA informs decision makers on the sources of uncertainty and provides information on the worth of investment resources in reducing uncertainty. In this way, PRA supplements traditional safety analyses that support safety-related decisions. Through the use of PRA, safety analyses are capable to focus on both the likelihood and severity of events and consequences that adversely impact safety.

PRA differs from reliability analysis in two important respects: (1) PRA allows a more precise quantification of uncertainty both for individual events and for the overall system, and (2) PRA applies more informative evaluations that quantify metrics related to the occurrence of highly adverse consequences (e.g., fatalities, loss of mission), as opposed to narrowly defined system performance metrics such as mean-time-to-failure. PRA also differs from hazard analysis, which identifies and evaluates metrics related to the effects of high-consequence and low-probability events, treating them as if they had happened; i.e., without regard to their likelihood of occurrence. Additionally, the completeness of the set of accident scenarios cannot be assured in the conduct of a hazard analysis. PRA results are more diverse and directly applicable to resource allocation and other RM decision-making based on a broader spectrum of consequence metrics.

Through the PRA process, weaknesses and vulnerabilities of the system that can adversely impact safety, performance, and mission success are identified. These results in turn provide insights into viable RM strategies to reduce risk and direct the decision maker to areas where expenditure of resources to improve design and operation may be more effective.

The most useful applications of PRAs have been in the risk evaluation of complex systems that may result in low-probability and high-consequence scenarios or the evaluation of complex scenarios consisting of chains of events that collectively may adversely impact system safety more than individually.

1 Scope

This standard supports and complements the implementation of the risk management process defined in ISO17666 in situations when application of quantitative risk assessment is deemed necessary. This standard defines the principles, process, implementation, and requirements for conducting a quantitative risk assessment and explains the details of probabilistic risk assessment (PRA) as applied to safety. While PRA can be applied to project risk management involving cost and schedule, this application is outside the scope of this standard.

This standard provides the basic requirements and procedures for use of PRA techniques to assess safety or mission risk and success in aerospace programs and projects. The standard is applicable to all international space projects involving: (1) the design of space vehicles for the transportation of personnel in space; (2) the design of space and non-terrestrial planetary stations inhabited by human being; (3) the design of space and launch vehicle powered by or carrying nuclear materials and (4) others projects as directed by authorities or clients. These types of projects generally involve scenarios, chains of events, or activities that could result in the death or serious injury to the public, astronauts or pilots, or the workforce; or the loss of critical or high-value equipment and property. For other types of projects, PRA is recommended but should be performed at the discretion of the project management.

2 Normative references

The following normative documents contain provisions, which through reference in this text constitute provisions of this ISO Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this ISO Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

ISO/DIS 14300-1	Space systems – Programme management – Part 1: Structuring the programme
ISO/DIS 14300-2	Space systems – Programme management – Part 2: Product Assurance
ISO/DIS 14620-1	Space systems – Safety requirements - Part 1: System safety
ISO/CD 16192	Space Systems – Lessons learned – Principles and rules
ISO/DIS 17666	Space systems – Risk management

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

The definitions given in ISO17666 apply. The following terms and definitions are specific to this Standard in that they are complementary or additional to those contained in ISO17666.

The definitions listed here comprise the terms used in the body of this standard.

3.1.1

acceptable risk

risk that is acceptable to program/project manager(s) and to stakeholders.

3.1.2

expert judgment

systematic and structured elicitation of likelihood data through estimation and assessment by a specialist

NOTE1 Structured implies the use of a method, systematic means regularly.

NOTE2 Mathematical aggregation of individual judgements is generally preferred over behavioural or consensus aggregation.

3.1.3

likelihood

probability of occurrence or the measure for the occurrence rate or frequency of an event, a hazard scenario or consequence.

3.1.4

likelihood reference frame

a relative indicator against which the likelihood is expressed.

NOTE1 The likelihood reference frame is linked to the structure of the analysis. A typical reference frame in use in space projects is "per mission".

3.1.5

risk

undesirable situation or circumstance that has both a likelihood of occurring and a potential consequence

NOTE1 Risks arise from uncertainty due to a lack of predictability or control of events. Risks are inherent to any project and can arise at any time during the project life cycle; reducing these uncertainties reduces the risk.

NOTE2 This definition is given in ISO17666.

3.1.6

risk contributor

a single event or a particular set of events upon which the risk depends

NOTE1 Risk contributors can be ranked relative to each other by their *risk contribution.*

3.1.7

risk contribution

a measure of the decrease of the likelihood of a top consequence, when the events associated with the corresponding risk contributor are assumed not to occur.

NOTE1 Risk contribution indicates (is directly proportional to) the *risk reduction potential* of the risk contributor. Important risk contributors are events, which have a high-risk contribution and risk reduction potential.

NOTE2 Risk contribution provides a systematic measure that makes it possible to rank design and operation constituents of a system from a safety risk point of view. It allows the identification of high risk or vulnerable areas in the system, which can then serve as drivers for safety improvements.

3.1.8

safety risk

a measure of the impact on safety posed by hazard scenarios and their consequences.

NOTE1 Safety risk is always associated with a specific hazard scenario or a particular set of scenarios. The risk posed by a single scenario is called *individual scenario risk*. The risk posed by the combination of individual risks and their impact on each other is called *overall risk*.

NOTE2 The magnitude of safety risk is represented by the severity and the likelihood of the consequence.

3.1.9

scenario

refer to ISO 17666

3.1.10

stakeholder

someone or an organization that stands to gain or to lose as a result of risk consequences

3.1.11

uncertainty

the range of likelihood due to randomness, imprecision, lack of data/information and the lack of understanding of the systema and its response

NOTE1 Uncertainty can be represented as an interval with an upper and lower value or as an uncertainty distribution.

3.1.12

uncertainty contributor

a single event or a particular set of events upon which the uncertainty of the top consequence depends

NOTE1 Uncertainty contributors can be ranked relative to each other by their *uncertainty contribution.*

3.1.13

uncertainty contribution

a measure of the decrease of the uncertainty of a top consequence, when the likelihoods of the events associated with the corresponding uncertainty contributor are assumed to be without uncertainty.

NOTE1 Uncertainty contribution indicates (is directly proportional to) the *uncertainty reduction potential* of the uncertainty contributor. Important uncertainty contributors are events, which have a high uncertainty contribution and uncertainty reduction potential.

NOTE2 Uncertainty contribution provides a systematic measure that makes it possible to rank data and information sources.

3.2 Abbreviated terms

For the purposes of this document, the following terms are defined and apply:

PRA	Probabilistic Risk Assessment
P(A)	probability of event A
P(A/B)	conditional probability of event A given event B has occurred

4 Principles of probabilistic risk assessment

Probabilistic risk assessment (PRA) assists engineers and managers to include risk results in management and engineering practices and in the decision making process throughout a project life cycle for such aspects as design, construction, testing, operation, maintenance, and disposal, together with their interfaces, management, cost and schedule (ISO17666).

Probabilistic risk assessment supports and interfaces with the risk management process by providing the required relevant risk data. Risk management and risk assessment complement each other.

The steps in the risk management process as described in ISO17666 are given below.

1. Define risk management implementation requirements
2. Identify and assess the risks
3. Decide and act
4. Monitor, communicate and accept risks
5. Control of residual risks

The second step, above, (Identify and assess the risks) is a process also called *risk assessment*. Once step 1 is completed, risk assessment provides the information used to conduct the remainder of the risk management process. Risk assessment provides the data to base decisions concerning the design and implementation of controls used to prevent or mitigate risks.

The third step includes the opportunity to decide whether the assessed risk is acceptable to program/project management and the stakeholders. If the risk is unacceptable, measures must be taken to bring it down to an acceptable level. If it is acceptable, management measures must be taken (steps 4 and 5) to monitor the evolution of risk and to ensure that it will not grow to unacceptable levels.

Risk assessment can be performed qualitatively or quantitatively or both. Qualitative risk assessment is performed by categorizing the likelihoods and consequences of risk as discussed below, where it applies to safety problems. In this context, it is called safety risk assessment.

In many cases, likelihoods and consequences need to be evaluated quantitatively. If sufficient statistical data do not exist for this purpose, modelling techniques are used.

For rare (very low probability) events, where sufficient statistical data do not exist, the significance of important risk drivers is assessed through a process called probabilistic risk assessment (PRA) is used. The PRA process will be discussed in a later section of this standard.

In the rest of this document, PRA methodology primarily intended for safety applications is discussed. Another form of risk assessment, called “Programmatic Risk Assessment” is used to assess the risks of not performing within pre-defined program schedule and cost estimates. In this process, schedule profiles based on uncertainties in the originally defined schedule are modeled using simulation or Monte Carlo methods. These uncertainties can occur due to a number of technical or management reasons. Subsequently, the effects of schedule changes and of other technical or management impacts on cost are evaluated. Programmatic risk is then evaluated in the form of distributions of probabilities of exceeding given schedule milestones and costs.

4.1 Safety risk assessment concept

The application of PRA to safety problems is discussed here. The safety risk assessment concept is derived from probabilistic risk assessment (PRA). Safety risk assessment complements deterministic hazard analysis by adding a probabilistic dimension to the evaluation of hazards in support risk informed decision-making. The probabilistic dimension is expressed in terms of likelihoods.

The interface between safety risk assessment and hazard analysis is shown in Figure 1.

Safety risk assessment can be used to either assess the risks posed by individual hazard scenarios separately, or assess sets of scenarios, collectively, in the form of the overall risk posed by those scenarios.

The assessment of individual scenarios can be performed using consequence severity and scenario likelihood categorization schemes by applying risk grids or risk matrices and risk indexes, as described in ISO/DIS 17666.. However, these risk matrix and index methods cannot be used to combine individual component of risk within a scenario or combine scenarios to evaluate overall risk. These methods do not constitute combinatorial computational tools.

Assessment of the overall risk posed by a particular set of scenarios requires the rigor of the PRA approach. This assessment provides the basis for identifying and ranking risk contributors. Important contributors can then be used for driving and optimizing the system design or operation from a safety performance point of view. The calculated overall risk can also be compared to probabilistic safety targets or acceptance criteria. Acceptable risks are defined by Authorities or client in Step 1 of the risk management process. Risk can also be used as a metric for quantifying safety in decision models.

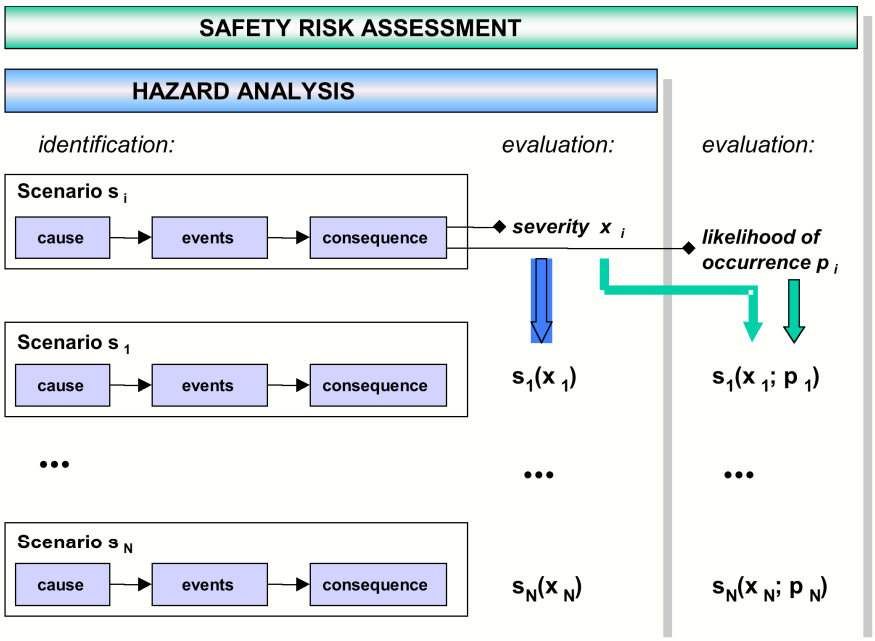

Figure 1: Interface between safety risk assessment and hazard analysis

A representation of the assessment of overall safety risk is shown in Figure 2. As indicated in the figure, safety risk assessment uses hazard scenarios to model individual sequences of events that are *necessary and sufficient* for an undesired system level consequence to occur. A scenario can be represented as a "*logical intersection*" of the initial cause or initiating event and the necessary conditional intermediate events leading to the associated consequence. The overall risk is then the *logical union* of the risk of the individual scenario that lead to same consequence.

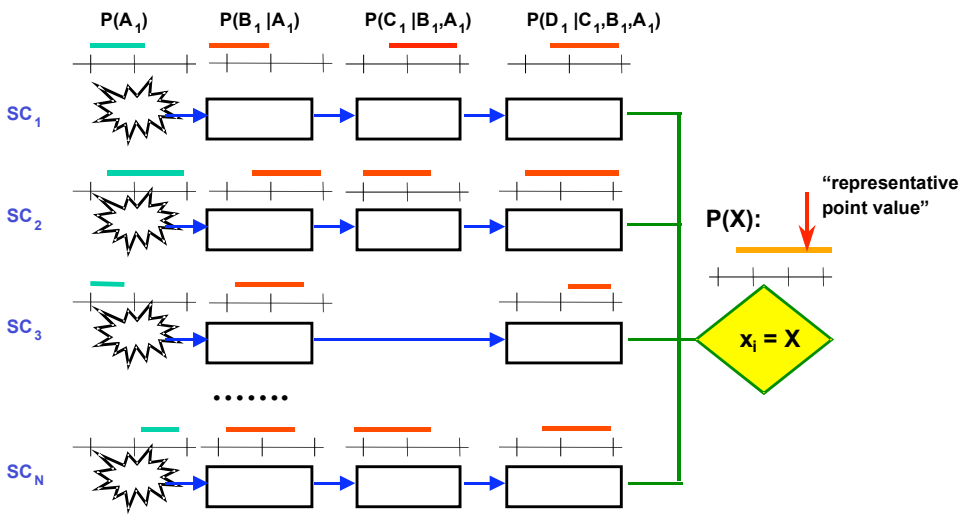

Figure 2: Example of the assessment of the overall risk

Probabilistic risk assessments of complex systems identify scenarios typically using event trees or event sequence diagrams and fault trees to derive the logical models that lead to particular undesired safety consequences of interest. As described above, to quantify scenarios, the likelihood of the initiating events (i.e. causes) and the probability of each subsequent intermediate event, conditional on the occurrence of the previous events in the sequence, are combined to determine the probability that the end state (i.e. consequences) will occur. For each scenario, the severity (i.e. magnitude) of the consequences is usually determined based on the physical characteristics and nature of the scenario being evaluated. The overall consequences are determined by summing over all scenarios in a process that is analogous to that used to determine the overall probability

An estimation of event likelihoods is usually based on different sources of data. Typical data sources include: previous experience with the particular system [i.e. measured or directly observed relevant test or experience data and lessons learned (see 16192], data from other systems or projects (i.e. extrapolation from generic data, similarity data, or physical models), and expert judgment (i.e. direct estimation of likelihoods by domain specialists). Events are quantified in the context of the corresponding hazard scenario, i.e. the likelihood of an event is assessed conditionally on the previous events in the sequence.

Systematic identification and treatment of uncertainties is characteristic to the assessment of the overall risk and conducted in two ways. The likelihood estimates of scenario events are produced with their associated uncertainties, and presented in the form of probability distributions or intervals. These uncertainties are then propagated in the calculations of the likelihoods of the consequence(s).

Quantification of the overall risk is obtained by calculating the likelihoods and magnitudes of the consequences. This calculation can be achieved through the use of point values or probability (uncertainty) distributions. An uncertainty distribution is characterized by representative point values, e.g. the mean or a specific quintile value in the upper part of the distribution. A representative point value in the upper part of the uncertainty distribution associated with the overall risk, at a confidence level accepted by the decision maker, tends to be used to implement the precautionary principle for risk acceptance decisions and for risk comparisons. The precautionary principle implies that conservative assumptions with respect to the risk value are preferred to optimistic ones to ensure that a system is not considered to satisfy an agreed risk target or an acceptance criterion falsely, or that one option is not falsely preferred to another one in the comparisons. Higher uncertainty regarding the overall risk value transfers a higher representative point value to be used for risk acceptance or comparisons.

The relative importance of an event or a scenario to the overall risk is measured by its risk contribution. The risk contribution provides information on the potential for safety improvement, i.e. potential for reducing the overall risk associated with the event or scenario. Similar to individual events, design and operation constituents can also be ranked from a risk reduction point of view by accumulating the risk contributions of the events associated with the particular constituents.

The relative importance of the uncertainty of an event or a scenario to the uncertainty of the overall risk is measured by its uncertainty contribution. Uncertainty contribution values indicate and rank those events, which are the main sources of uncertainty for the consequence likelihood, and have the highest potential for the reducing this uncertainty. Reduction of consequence uncertainties directly transfers to the use of lower representative point values of the consequence likelihoods.

Risk and uncertainty contributors are identified based on their ranking. Important risk and uncertainty contributors are those events, or their corresponding system constituents, that have high-risk reduction and uncertainty reduction potential.

4.2 Concept of risk and probabilistic risk assessment

The concept of risk includes both undesirable consequences, e.g., the number of people harmed, and the probability of occurrence of the consequences. Sometimes, risk is defined as the expected value of consequence occurrence. This representation of risk results in a summary measure and not a

general definition. Understanding how the system fails and producing probability distributions for the consequences affords a much more complete description of risk.

A common definition of risk is represented by a set of triplets. Determining risk generally amounts to answering the following questions:

1. What can go wrong? (the scenario)
2. How likely is it? (likelihood)
3. What are the consequences? (severity of the consequences)

The answer to the first question is a set of accident scenarios. The answer to the second question requires evaluating the probabilities that the scenarios will occur and the answer to the third question requires estimating associated consequences. In addition to probabilities and consequences, the triplet definition emphasizes the development of accident scenarios and makes them part of the definition of risk. These scenarios are indeed one of the most important results of a risk assessment. Figure 3 illustrates the implementation of these concepts in PRA.

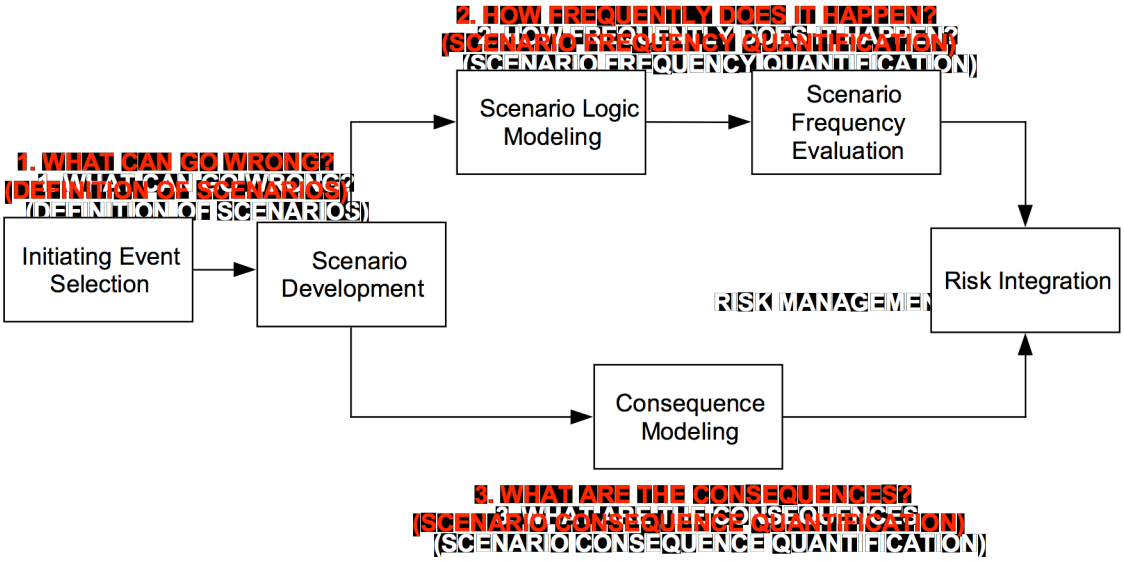

Figure 3: Implementation of the Triplet Definition of Risk in PRA

The PRA process begins by identifying a set of “initiating events” (IEs) that perturb the system (i.e., adverse triggers that cause it to change its operating state or configuration). For each IE, the analysis proceeds by determining the subsequent events (failures) that can lead to undesirable consequences. Then, the magnitudes of the consequences of these scenarios are determined, as well as their occurrence frequencies (probabilities). Finally, frequencies and consequences are integrated into a representation of the risk profile of the system. This risk profile is then used to support risk management decisions.

5 Objectives, uses, and benefits of probabilistic risk assessment

The objectives of a probabilistic risk assessment are to:

– identify and assess the (safety or mission) risks posed by individual identified scenarios, or identify and assess the overall risk posed by sets of scenarios, collectively;

– identify risk and uncertainty contributors, and corresponding risk areas in system design and operation;

– rank risk and uncertainty contributors in a decreasing order of importance; and

– identify and prioritise options for risk reduction.

Probabilistic Risk Assessment results are used to:

- assess the level of safety or mission risk and success in a quantitative (probabilistic) manner;
- decrease the level mission risk and increase the level of safety or mission success of a system through risk reduction;
- drive the definition and implementation of design and operational requirements, specifications, concepts, procedures etc.;
- provide a quantitative basis for defining safety and mission requirements by:
  - determining the applicability of safety and mission requirements,
  - implementing safety and mission requirements,
- verify PRA results implementation, and demonstrate compliance or non-compliance;
- support safety and mission-related project decisions;
- support safety submissions and reviews through documented evidence;
- support safety certification of a system through documented evidence;
- support risk communication and tracking; and
- provide input to overall project risk management.

The benefits of a probabilistic risk assessment are to:

- provide a quantitative framework for assessing risks and determining which are acceptable and which are not.
- apportion safety responsibilities among teams more realistically;
- allocate safety improvement expenditures in proportion with the impact of these improvements on risk reduction
- build safety into the system in an efficient and consistent way;
- quantitatively display the significance of accident scenarios;
- quantitatively identify system and component weaknesses;
- assess phase related system or subsystem safety levels; and
- quantitatively compare the efficiency of risk reduction actions.

The specific objectives of risk assessment with respect to a project specific application are determined under Task 1 of the risk assessment process.

6 PRA requirements and process

6.1 Probabilistic risk assessment requirements

The following probabilistic risk assessment requirements are defined:

a. Probabilistic risk assessment shall follow the process as defined in the sub clause 6.3;

b. Probabilistic risk assessment shall be documented in accordance with the requirements of clause 8 Probabilistic risk assessment reports – document content requirements.

6.2 Overview of the probabilistic risk assessment process

The tasks of a probabilistic risk assessment described below are used to address Step 2 of the risk management process as discussed in Section 4.1 of this standard and shown in Figure 4.

6.3 Probabilistic risk assessment tasks

The PRA task flow is shown in Figure 4. The following provides a brief description of each task.

Task 1: Objectives Definition

The initial task of a PRA is to define the objectives and scope of the analysis. The objectives of the risk assessment provide clear statements of the purpose and expected end uses for the results. The scope defines the mission profile and system(s) or portion thereof that will be included in the analysis. These two elements provide the basis for identifying and selecting the consequence(s) metrics of interest. These consequence metrics can include harm to humans (e.g., injury, illness, or death), degradation of mission capabilities, loss of mission, property damage and losses, or other undesired outcomes.

Depending on the objectives and scope of the PRA, applicable system configurations and time frame, guidelines for considering initiating events (i.e., whether to include external events such as micrometeoroids) should be defined. The results of Task 1 should be completely reviewed by the appropriate project management and responsible safety and mission assurance organizations prior to commencing with the assessment.

The following activities are included in Task 1:

a. Identify the objectives of the probabilistic risk assessment (by defining the intended purpose and use(s) of the analytical results).

b. Identify the scope and depth of the analysis [by defining the mission envelope, applicable systems boundaries (which part of systems design & operations will be analysed), and define the level of detail for accident scenarios and the associated analyses].

c. Identify the consequence metric(s) for the analysis including the consequence types and whether risks are required for individual hazard scenarios and/or overall risks of specific undesired consequences types (i.e., loss of mission, loss of vehicle, loss of crew):

    1. Identify the risk grid, index scheme or risk matrix to be used (based on consequence severity and scenario likelihood categories), and

    2. Identify specified overall risk targets or acceptance criteria (based on probabilistic targets and criterion for a specific consequence).

d. Identify associated information and data sources.

Task 2: System Familiarization

Familiarization with the system under analysis is the next step. Familiarization covers all relevant design and operational information, including engineering and process drawings, as well as operating and emergency procedures. If the PRA is being performed on an existing system that has been operated for some time, the engineering information must be on an as-built or as-operated basis. If the PRA is being conducted during design, the engineering information needed for the assessment is based on the as-designed configuration with considerations for system operations. Examination and, if possible visual inspection of the system(s) being analyzed, are recommended. The purpose of this effort is to become thoroughly familiar with the mission and systems involved and to gain an understanding of the success states and success criteria needed for proper overall mission completion. System familiarization identifies how the systems operate, their interdependencies, the role of the human in operations (command and control, maintenance) and any system configuration changes that may occur during applicable mission stages, phases or regimes. Mission and system success criteria provide the basis for developing functional and systemic models.

The following activities are included in Task 2:

a. Identify and describe the analytical scope, systems configuration and operation (functional and physical architecture and layout vis-à-vis the mission timeline) including mission phases and operating configurations, system constituents and functions, and physical zones, etc.

b. Define the mission success criteria along with contributions from and the success criteria of each system required for completion of the mission.

Task 3: Initiating Event Identification

Next, a complete set of initiating events that triggers subsequent accident scenarios must be identified and analyzed. These events initiate accident sequences leading to defined end states (consequence metrics). There are several ways to identify initiating events. If the PRA is being performed on an existing system that has been operated for some time, a review of passed experiences, incidences, and operating history can help identify initiating events. If the analysis is being conducted on new designs, past experience of similar systems in similar environments or with similar mission envelopes can be used. Along with experience data, systematic methods, such as Master Logic Diagrams (MLD) and Failure Modes and Effects Analysis (FMEA), are recommended for identifying initiating events. An MLD is a hierarchical, top-down tree display, showing general types of undesired events at the top, proceeding to increasingly detailed event descriptions at lower tiers, and displaying postulated initiating events at the bottom. A FMEA systematically assumes component failures and evaluates their effects on system performance.

When multiple initiating events leading to scenarios with the same end state are identified, those events having very low probabilities can be screened out. Independent initiating events can be grouped according to the similarity of challenges they pose to the system (i.e., initiated events that result in the same system response). When initiating events are treated as a group, their frequencies can be summed to derive the group initiator frequency.

The following activities are included in Task 3:

a. Identify and evaluate initiating events that can trigger subsequence accident scenarios using experience data and systematic methods (use relevant input from existing hazard analysis produced in accordance with MLDs and FMEAs),

b. Evaluate the occurrence probabilities of the identified initiating events and screen out those events with very low relative probabilities (or frequencies), and

c. Combine initiating events with similar effect on the system into groups and determine group occurrence probabilities (frequencies).

Task 4: Scenario Modelling

Modelling of accident scenario is an inductive process that usually involves tools called event trees. An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (also called pivotal events or top events), until end states are reached. Event trees generally take into account the time sequence of pivotal or top events that represent the functional or systemic behaviour of the overall system. Sometimes, a graphical tool called an event sequence diagram (ESD) is used to describe an accident scenario, because this type of diagram lends itself better to engineering thinking than does an event tree. An ESD is logically equivalent to an event tree and must then be converted to an event tree for quantification. Another type of inductive modelling tool that can also be employed is a reliability block diagram.

The following activities are included in Task 4:

a. For each initiating event (or combined group of events), model the approximate time sequence and conditional response (success or failure) of the pivotal events (i.e., human actions, structure, systems, components) needed to prevent the initiating event from causing potential consequences;

b. For those accident sequences that are postulated to lead to potential consequences, evaluate the conditional physical (mechanistic) response of the system to the physical impacts of the initiating events as modified by identified preventative controls (i.e., human actions, structures, systems, components) and determine the magnitude and characteristics of the ensuing physical response (i.e., detonation, deflagration, loss of control, loss of oxygen, etc.); and

c. For those physical system responses that can lead to potential consequences, model the conditional response (success or failure) of the controls (i.e., human actions, structures, systems, components) available or designed to mitigate the potential consequences that can be cause by the physical system responses.

Task 5: Failure Modelling

The modelling of failure causes and faults (or their complements, successes) of each pivotal or event tree top event is a deductive process that usually involves tools called fault trees. A fault tree consists of three parts. The top part is the top event, which corresponds to the failure of a pivotal event (or event tree top event) in the accident scenario. The middle part consists of intermediate events (faults) that, in combination, cause failure of the event immediately above it. These events are linked through logic gates (e.g., AND gates and OR gates) to the events both above and to events at the bottom part of the fault tree, called the basic events. There can be many layers of intermediate events to describe the failure of the pivotal (or top event). The occurrence of the basic events will ultimately lead to the occurrence of the top events through the logic of the fault tree. The fault trees are then linked to the accident scenarios and simplified (using Boolean reduction rules) to support quantification. Other deductive modelling tools can also be employed to evaluate the failure of top events.

The following activities are included in Task 5:

a. For each pivotal or event tree top event, identify and record the associated initiating event and previous events in the accident scenario. These events provide the initial and boundary conditions needed to evaluate their failure (or their complements, successes). In addition, record the success criteria (defined in Task 2) for the functioning the pivotal or top events that are also needed for the evaluation;

b. For each pivotal or event tree top event, develop the failure (i.e., fault tree) model; the logical combination of intermediate faults that can cause the top event. Dependent on the function or system being modelled, there may be several layers of intermediate events;

c. Identify the basic events (failures or faults) along with their success criteria for the initial and boundary conditions associated with the top event; and

d. Link the fault tree models for the pivotal or event tree top events to the associated portion of the event tree model.

Task 6: Quantification

Quantification refers to the process of estimating the frequency of occurrence and the magnitude of the consequences of the undesired end states for the accident scenarios. The frequency of occurrence of each end state is calculated using the fault tree linking approach resulting in the logical product of the initiating event frequency and the (conditional) probabilities of each pivotal event along the event sequence path from the initiating event to the end state. The failure models [fault tree(s)] for the pivotal events provide the logical combinations of basic events needed for the quantification of the pivotal events (through the linking process). The magnitudes of the undesired end states (consequences) for the accident sequences are usually evaluated through deterministic calculations taking into account the physical response of the system being evaluated and the functioning of the systems identified or designed to mitigate the consequences. All sequences with like end states are then grouped; i.e., their probabilities are logically summed into the probability of the representative end state.

The following activities are included in Task 6:

a. Perform the Boolean evaluation of the linked event sequence [event tree(s)] and failure models [fault tree(s)] for each initiating event. This evaluation will result in sets of basic events (called minimal cut sets) leading to the undesired end states. These minimal cut sets represent the accident sequences in terms of the basic events;

b. Estimate the frequency of occurrence of each minimal cut set by logically combining the initiating event frequency with the failure probabilities for the associated basic events; Typical data sources for the failure probabilities include: previous experience with the particular system (i.e. measured or directly observed relevant test or experience data and lessons learned), data from other systems or projects (i.e. extrapolation from generic data bases, similarity data, or physical models), and expert judgement (i.e. direct estimation of likelihoods by domain specialists).

c. Estimate the type and magnitude of the consequences; and

d. Group the sequences with the same end state and logically sum their probabilities to estimate an overall probability that each representative end state will occur.

Task 7: Uncertainty Analysis

One purpose of a PRA is to develop realistic models that take into account the uncertainty in events. Therefore, the probabilistic risk model is effectively an uncertainty analysis model. Recognizing that uncertainty analysis is a main constituent of the probabilistic risk model and assessment provides the foundation to the proper application of the PRA results in the RM decision-making process. It is incumbent on the PRA analyst to find ways to quantify and present uncertainties associated with analytical inputs, models and degree of knowledge in a manner that will make the risk results understandable and usable to the decision-makers. All PRA insights reported to decision-makers should include an appreciation of the overall degree of uncertainty involved and provide insights concerning which sources of uncertainty are critical to the results. Monte Carlo simulation methods are generally used to perform uncertainty analysis.

The following activities are included in Task 7:

a. When estimating the frequency of occurrence of each minimal cut set, the uncertainty in the data should be included. Develop appropriate uncertainty distributions or representations for the basic events in the minimal cuts sets;

b. Logically combine the uncertainty distribution for the initiating event with the uncertainty distributions for the failure probabilities associated basic events. There are a number of methods available for performing these calculations including analytical methods and Monte Carlo simulation;

c. Determine uncertainties in the magnitude of the undesired end states (consequences);

d. Evaluate the uncertainty contribution of individual basic events to the uncertainty in the overall results; and

e. Record the results with their uncertainty bounds including insights concerning which sources of uncertainty are critical to the results.

Task 8: Sensitivity Analysis

Sensitivity analysis is a type of uncertainty analysis that focuses on evaluating the effects of variations (due to uncertainties) in assumptions, modelling, physical parameters and basic events. These analyses are frequently performed in a PRA to indicate those analytical inputs or elements whose changes in value cause the greatest changes in partial or final risk results. Sensitivity analyses are also used to assess the sensitivity of the PRA results to dependencies among basic event failures.

The following activities are included in Task 8:

a. List the assumptions concerning: mission, structure, system and component success criteria; modelling; and physical parameters. In addition, identify those structures, systems and components contained in single accident sequences (minimal cuts sets) that have a common property, which could render them susceptible to dependent failures;

b. For the assumptions, systematically and independently vary the success criteria, modelling, and parametric values, and change the PRA models and data by adjusting the event sequence [event tree(s)] and event failure models [fault tree(s)] appropriately. Re-evaluate the overall PRA model for changes in the accident sequences, ranking and quantitative risk results; and

c. For potentially dependent structures, systems and components within a single cut set; combine them into a single basic event and assign it the highest probability among the coupled events. Independently re-evaluate the overall PRA model for changes that occur to the accident sequences, ranking and quantitative risk results from each adjusted cut set.

Task 9: Ranking

In some PRA applications, special techniques are used to identify the lead, or dominant, contributors to risk in accident sequences or scenarios. The ranking of these lead or dominant contributors in decreasing order of importance is called importance ranking. The ranking process is usually

performed using the event sequence [event tree(s)] and event failure models [fault tree(s)]. There are several quantitative importance measures that typically determine the change in the quantified risk (probability) due to the change in the probability of a basic event or measure the contribution of a basic event to the overall risk. Some of these quantitative important measures include; Fussell-Vesely (F-V), risk reduction worth (RRW), risk achievement worth (RAW), and Birnbaum.

The following activities are included in Task 9:

a. Identify the main risk contributors:

b. Evaluate the overall risk model for the selected importance measures and rank order individual accident scenarios and basic events accordingly; and

c. Determine the contributions to the overall risk and uncertainty from these accident sequences and basic events.

Task 10: Data Analysis

Data analysis refers to the process of collecting and analyzing information and data in order to estimate various parameters of the initiating events and the basic events used in the PRA models. These parameters are normally organized into a database and used to obtain probabilities for structures, systems, and component failure rates; initiator frequencies; human failure probabilities and common cause factors. In cases where there are no statistically significant data to support PRA parameter estimation, the PRA analyst may need to rely on expert judgment and elicitation. The data collection and analysis task proceeds in parallel or in conjunction with the steps described above

The following activities are included in Task 10:

a. Identify the data needed from the initiating events and the basics events in the PRA model;

b. Collect likelihood information and data for the events from objective data (measured or directly observed from relevant test or experience), semi-objective data (extrapolation from generic data, similarity data, or physical models); and subjective data (expert judgment by domain specialists);

c. Estimate event probabilities using statistical methods and develop uncertainty distributions, and

d. Developing a PRA database containing collected information and data, parameter estimates, and probabilities including uncertainties.

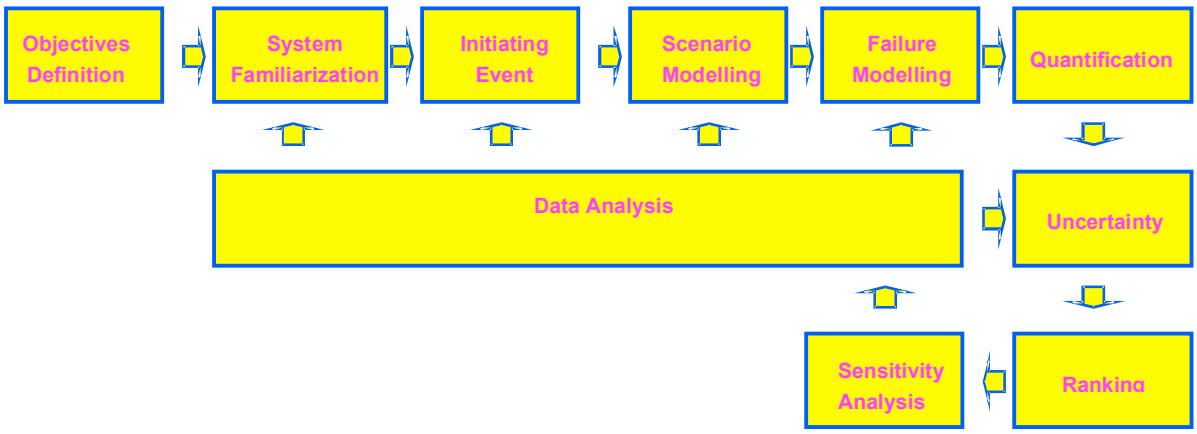

Figure 4: Task flow in a typical PRA

7 Peer Review

In order to enhance the quality and credibility of a PRA, internal and external peer reviews should be conducted. In general, these reviews concentrate on the appropriateness of methods, information, sources, judgments, and assumptions as well as their application to the project being evaluated and its objective(s).

The purpose of these reviews is to verify the correct application of the methodology and the accuracy of the analytical results. Peer reviews should be conducted for all PRAs.

7.1 Internal Peer Reviews

Internal reviews are conduct by team members to crosscheck each other's models and results. These reviews also involve examination and discussions of the models and results with individuals most knowledgeable with the systems being evaluated including designer, builders and operators; whoever applies.

7.2 External Peer Reviews

This type of review is carried out by independent peers, i.e., people who are not involved in the study and have no stake in it but have capabilities that are better than those of the individuals who performed the study. The peers' expertise should span the range of disciplines and experience required for the study.

The use of a participatory peer review should be considered. The participatory peer review process begins early in the assessment and proceeds in parallel with the project involving frequent, periodic contact and interactions with the PRA team. This type of review is conducted in order to identify problems and to recommend corrective actions early, instead of waiting to begin the peer review when the PRA is virtually complete. While this approach may sacrifice some independence in the peer review, it is likely to result in a PRA performed correctly the first time saving expenditure of time and resources to correct problems at the end of the project.

8 Probabilistic risk assessment report - data content requirements

This clause establishes the data content requirements for a Probabilistic Risk Assessment report, as shown in the table below. The safety risk assessment report may be combined with a hazard analysis report as appropriate.

Probabilistic risk assessment report contents	
Main Clause	**Description**
Title Page	The title page shall include: Document title, document number and release date, Name and affiliation of author (s) and release signatures
Document Change Record	The document change record shall be completed in accordance with project configuration management requirements
Table of Contents	Self explanatory
Introduction/	This clause shall provide a brief introduction of the

Probabilistic risk assessment report contents	
Main Clause	**Description**
Scope/Summary	report, its scope and a summary of the main findings.
Documents	This clause shall provide a list of all applicable (normative) and reference (informative) documents used to establish the report.
Terms, Definitions and Acronyms	Terms, definitions and acronyms shall be explained. Unless they are unique to the report, this may be by reference to other documents.
Scope, Mission Profile, and Systems	This clause shall provide the scope, the mission profile and system(s) or portion thereof, included in the analysis.
Requirements	This clause shall provide a summary of the relevant requirements on the systems under consideration and on the performance of the assessment including consequence severity and scenario likelihood categorizations.
Assumptions,	This clause shall provide a description of any assumptions made in performing the assessment, including, where necessary, any limitations on the performance of the assessment (e.g. not all tasks performed…)
Description of the System/Functions	This clause shall provide a description of the systems and functions in sufficient detail to support the modelling and findings of the assessment.
Description of the Methods, Models, and Analytical Techniques	This clause shall provide a description of the methods and models used in performing the analysis, including, where applicable, the analytical techniques for systems response and consequence quantification.
Data Analysis	This clause shall provide a description of the data, data reduction techniques and uncertainty models used in the assessment.
Summary of Results and Recommendations	This clause shall summarise the results of the assessment and provide recommendations

Bibliography

The following documents can be consulted for further reading on risk analysis / assessment:

[1] ECSS-M-00-03 *Space project management - Risk management*

[2] ECSS-Q-40-03 *Space product assurance – Safety risk assessment (draft)*

[3] NASA NPG 7120.5 *NASA program and Project Management Processes and Requirements*

[4] NASA NPG 8700.4 *Risk management procedures and guidelines*

[5] NASA NPG 8705.4 *Probabilistic risk assessment procedures and guidelines*

[6] ESA *"Handbook & Procedure Guide for Risk Management" RIMOX: http://www.estec.esa.nl/qq/RIMOX/Default.htm*

[7] *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practioners. Version 1.1, August 2002. NASA Headquarters, Office of Safety and Mission Assurance*

[8] IEC 60300-3-9 "Risk Analysis of Technological Systems"

[9] *Probabilistic Risk Assessment, Procedures Guide for NASA Managers and Practitioners, Version 1.1(August 2002)*

[10] *Fault Tree Handbook with Aerospace Applications, Version 1.1 (August 2002).*